

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平8-186569

(43)公開日 平成8年(1996)7月16日

(51)Int.Cl.⁶

識別記号

庁内整理番号

F 1

技術表示箇所

H 0 4 L 12/28

G 0 6 F 13/00

3 5 5

7368-5E

H 0 4 L 11/ 00

3 1 0 D

審査請求 未請求 請求項の数 4 O L (全 16 頁)

(21)出願番号

特願平6-326436

(22)出願日

平成6年(1994)12月27日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 網 淳子

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(72)発明者 岡本 利夫

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

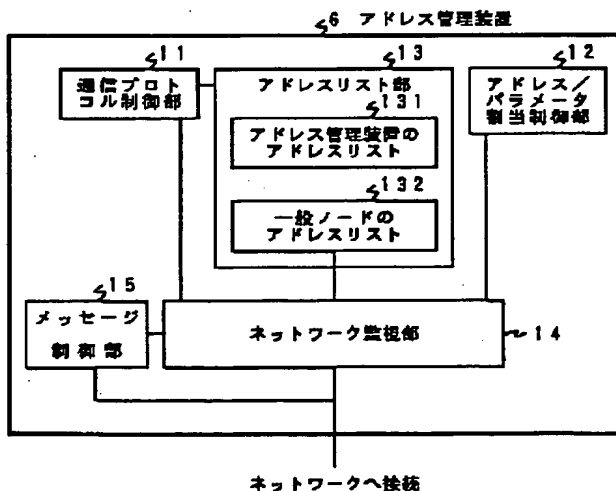
(74)代理人 弁理士 鈴江 武彦

(54)【発明の名称】 アドレス管理装置およびアドレス管理方法

(57)【要約】

【目的】 不正なアドレス管理装置および不正な端末装置の存在を監視することのできるアドレス管理装置および方法を提供することを目的とする。

【構成】 ネットワークに接続された各ノードからの要求に応じネットワーク層アドレスを割当てるアドレス管理装置において、ネットワーク層アドレスとデータリンク層アドレスを組にして記憶するアドレスリストと、ネットワーク上を伝送されるパケットをその宛先にかかわらず受信する受信手段と、受信したパケットから、該パケットの発信元ノードのネットワーク層アドレスとデータリンク層アドレスの組または宛先ノードのネットワーク層アドレスとデータリンク層アドレスの組の少なくとも一方を抽出する抽出手段と、抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組が、アドレスリストに記憶された組の中に存在するか否かを判定する判定手段とを備えたことを特徴とする。



1

【特許請求の範囲】

【請求項1】 ネットワークに接続された各ノードからの該ノードに固有のデータリンク層アドレスに基づくアドレス割り当て要求に応答して該ノードがパケット通信に用いるネットワーク層アドレスを割り当てるアドレス管理装置において、

既に割り当てられたネットワーク層アドレスと、対応するデータリンク層アドレスを組にして記憶するアドレスリスト記憶手段と、

ネットワーク上を伝送されるパケットをその宛先にかかわらず受信する受信手段と、

受信したパケットから、該パケットの発信元ノードのネットワーク層アドレスおよびデータリンク層アドレスの組または宛先ノードのネットワーク層アドレスおよびデータリンク層アドレスの組の少なくとも一方を抽出する抽出手段と、

抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組が、前記アドレスリスト手段に記憶された組の中に存在するか否かを判定する判定手段とを備えたことを特徴とするアドレス管理装置。

【請求項2】 ネットワークに接続された各ノードからのデータリンク層アドレスに基づくアドレス割り当て要求に応答して該ノードがパケット通信に用いるネットワーク層アドレスを割り当てるアドレス管理装置において、当該アドレス管理装置自身を要求元として、前記アドレス割り当て要求を疑似的に送出する手段と、

所定の時間が経過する間に、疑似的に送出した前記アドレス割り当て要求に対する応答パケットが伝送されてきた場合、該応答パケットの送信元ノードのネットワーク層アドレスおよびデータリンク層アドレスを抽出する抽出手段とを備えたことを特徴とするアドレス管理装置。

【請求項3】 ネットワークに接続された各ノードからのデータリンク層アドレスに基づくアドレス割り当て要求に応答して該ノードがパケット通信に用いるネットワーク層アドレスを割り当てるアドレス管理装置において、既に割り当てられたネットワーク層アドレスと、対応するデータリンク層アドレスを組にして記憶するアドレスリスト記憶手段と、

該アドレス管理装置自身を要求元として、前記アドレス割り当て要求を疑似的に送出する手段と、

所定の時間が経過する間に、疑似的に送出した前記アドレス割り当て要求に対する応答パケットが伝送されてきた場合、該応答パケットの送信元ノードのネットワーク層アドレスおよびデータリンク層アドレスを抽出する抽出手段と、

抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組が、前記アドレスリスト手段に記憶された組の中に存在するか否かを判定する判定手段とを備えたことを特徴とするアドレス管理装置。

【請求項4】 ネットワークに接続された各ノード間で、

2

アドレス管理装置により該ノード固有のデータリンク層アドレスに対して割り当てられたネットワーク層アドレスを用いて行うパケット通信を監視して、アドレス管理装置により割り当てられたものではないネットワーク層アドレスを用いる不正なノードを検出するアドレス管理方法であって、

前記アドレス管理装置は、

既に割り当てられたネットワーク層アドレスと、対応するデータリンク層アドレスを組にしてアドレスリストに登録し、

ネットワーク上を伝送されるパケットをその宛先にかかわらず受信し、

受信したパケットから、該パケットの発信元ノードのネットワーク層アドレスおよびデータリンク層アドレスの組または宛先ノードのネットワーク層アドレスおよびデータリンク層アドレスの組の少なくとも一方を抽出し、

抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組が、前記アドレスリストに登録された組の中に存在するか否かを判定することを特徴とするアドレス管理方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、ネットワーク間を移動するノードを許容するシステムにおいて、アドレス割り当ておよびそのセキュリティ保守を行うアドレス管理装置および方法に関する。

【0002】

【従来の技術】 コンピューターのパーソナル化に伴い、計算機を移動して様々な場所で使用する機会が増加している。ネットワークの通信プロトコルとしてネットワーク層アドレスに基づいて通信を制御するためのプロトコル、例えばTCP/IP、を用いる環境においては、計算機を物理的に移動し、以前と異なる接続点においてネットワークに接続した際、その新たに接続したネットワークにおいて使用可能なネットワーク層アドレス、例えばTCP/IPの場合はIP(Internet Protocol)アドレス、を手に入れる必要がある。

【0003】 ところで、このような操作をネットワーク管理者等、人手に頼ってはいは管理の手間もかかり、誤設定の可能性もあるので、自動的にネットワーク層アドレス(例えばIPアドレス)の割り当てと必要な各種パラメータの設定などを行う技術が提案されている。例えば、IETF(Internet Engineering Task Force)から公表されている文献RFC(Request For Comments)1533および文献RFC1541において示されているDHCP(Dynamic Host Configuration Protocol)などが良く知られている。

【0004】 しかしながら、このような技術を利用した

3

通信を実用化するにあたっては、悪意を持ったノードがネットワーク内に存在して他のノード間の通信を妨げることが容易にできてしまうなど、依然としてセキュリティ上の問題点が残されている。例えば、次のようなケースが考えられる。ネットワーク間を移動するノードは、通信を行うことを可能とするため、移動先でネットワーク層アドレスを取得する。このネットワーク層アドレスは、移動前に所属していたネットワークから付与されていたアドレスと同一である場合も異っている場合もある。従来技術では、通信のセキュリティが考慮されていないため、移動先でアドレスを取得する際にアドレス管理装置あるいはアドレス設定を行う者が故意または過失により不適切なアドレスを設定するおそれがある。また、不正なノードがアドレスを偽ってパケットを送信したり、正しいノードが送信したパケットを不正なノードが傍受したり、あるいは正しいノードがネットワークから切り離された後に不正なノードが傍受しておいたパケットを送信するといった通信のセキュリティを低下させる事態が発生するおそれがある。

【0005】

【発明が解決しようとする課題】 以上のように、従来のアドレス管理装置および方法では、故意に不適切なアドレスを設定するような不正なアドレス管理装置が出現し、あるいは不正にアドレスを設定してネットワークにパケットを送信したり、正しいノードが送信したパケットを傍受するような不正な端末装置が出現し、またはアドレス管理装置が過失によって不適切なアドレスを設定してしまった結果、不正なアドレスを持つ端末装置が出現しても、これを監視することはできなかった。

【0006】 本発明は、上記問題点に鑑みてなされたものであり、不正なアドレス管理装置および不正な端末装置の存在を監視することのできるアドレス管理装置および方法を提供することを目的とする。また、本発明は、不正なアドレス管理装置の存在を能動的に監視することのできるアドレス管理装置および方法を提供することを目的とする。

【0007】

【課題を解決するための手段】 第1の発明は、アドレス管理装置に登録されたノード（アドレス管理装置および一般ノード）であるか否かを基準として、ノードの正当性を判断することを可能にすることを特徴とする。

【0008】 すなわち、第1の発明は、ネットワークに接続された各ノードからの該ノードに固有のデータリンク層アドレスに基づくアドレス割り当て要求に応答して該ノードがパケット通信に用いるネットワーク層アドレスを割り当てるアドレス管理装置において、既に割り当てられたネットワーク層アドレスと、対応するデータリンク層アドレスを組にして記憶するアドレスリスト記憶手段と、ネットワーク上を伝送されるパケットをその宛先にかかわらず受信する受信手段と、受信したパケットが

4

ら、該パケットの発信元ノードのネットワーク層アドレスおよびデータリンク層アドレスの組または宛先ノードのネットワーク層アドレスおよびデータリンク層アドレスの組の少なくとも一方を抽出する抽出手段と、抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組が、前記アドレスリスト手段に記憶された組の中に存在するか否かを判定する判定手段とを備えたことを特徴とする。

【0009】 第2の発明では、アドレス管理装置が1台である場合に、管理用メッセージをネットワークに送出し、そのメッセージに対する応答の有無で、登録されていない不正なアドレス管理装置を検出することを特徴とする。

【0010】 すなわち、第2の発明は、ネットワークに接続された各ノードからのデータリンク層アドレスに基づくアドレス割り当て要求に응答して該ノードがパケット通信に用いるネットワーク層アドレスを割り当てるアドレス管理装置において、当該アドレス管理装置自身を要求元として、前記アドレス割り当て要求を疑似的に送出する手段と、所定の時間が経過する間に、疑似的に送出した前記アドレス割り当て要求に対する応答パケットが伝送されてきた場合、該応答パケットの送信元ノードのネットワーク層アドレスおよびデータリンク層アドレスを抽出する抽出手段とを備えたことを特徴とする。

【0011】 第3の発明では、アドレス管理装置が管理用メッセージをネットワークに送出し、そのメッセージに対する応答を検査することで、登録されていない不正なアドレス管理装置を検出することを特徴とする。

【0012】 すなわち、第3の発明は、ネットワークに接続された各ノードからのデータリンク層アドレスに基づくアドレス割り当て要求に응答して該ノードがパケット通信に用いるネットワーク層アドレスを割り当てるアドレス管理装置において、既に割り当てられたネットワーク層アドレスと、対応するデータリンク層アドレスを組にして記憶するアドレスリスト記憶手段と、該アドレス管理装置自身を要求元として、前記アドレス割り当て要求を疑似的に送出する手段と、所定の時間が経過する間に、疑似的に送出した前記アドレス割り当て要求に対する応答パケットが伝送されてきた場合、該応答パケットの送信元ノードのネットワーク層アドレスおよびデータリンク層アドレスを抽出する抽出手段と、抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組が、前記アドレスリスト手段に記憶された組の中に存在するか否かを判定する判定手段とを備えたことを特徴とする。

【0013】 第4の発明は、ネットワークに接続された各ノード間で、アドレス管理装置により該ノード固有のデータリンク層アドレスに対して割り当てられたネットワーク層アドレスを用いて行うパケット通信を監視して、アドレス管理装置により割り当てられたものではな

5

いネットワーク層アドレスを用いる不正なノードを検出するアドレス管理方法であって、前記アドレス管理装置は、既に割り当られたネットワーク層アドレスと、対応するデータリンク層アドレスを組にしてアドレスリストに登録し、ネットワーク上を伝送されるパケットをその宛先にかかわらず受信し、受信したパケットから、該パケットの発信元ノードのネットワーク層アドレスおよびデータリンク層アドレスの組または宛先ノードのネットワーク層アドレスおよびデータリンク層アドレスの組の少なくとも一方を抽出し、抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組が、前記アドレスリストに登録された組の中に存在するか否かを判定することを特徴とする。

【0014】第5の発明は、第1の発明または第2の発明のアドレス管理装置を同一の管理範囲内に複数台設置し、各アドレス管理装置が割り当てることのできるネットワーク層アドレスの値を、互いに重複しないように設定することを特徴とする。

【0015】第6の発明は、第1の発明または第2の発明のアドレス管理装置を同一の管理範囲内に複数台設置し、ネットワーク全体のアドレスリストを管理するデータベースを設け、各アドレス管理装置は、データベースに問い合わせを行ってネットワーク層アドレスの割り当てを行うとともに、各アドレス管理装置のアドレス要求に対する反応時間を、互いに異なる長さに設定することを特徴とする。

【0016】

【作用】第1の発明では、既に割り当られたネットワーク層アドレスと対応するデータリンク層アドレスを組にしてアドレスリスト記憶手段に記憶している。アドレス管理装置は、ネットワーク上を伝送されるパケットをその宛先にかかわらず受信し、受信したパケットから、該パケットの発信元ノードのネットワーク層アドレスおよびデータリンク層アドレスの組または宛先ノードのネットワーク層アドレスおよびデータリンク層アドレスの組の少なくとも一方を抽出する。抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組は、アドレスリスト手段に記憶された組の中に存在するか否かを判定される。

【0017】ネットワーク層アドレスおよびデータリンク層アドレスの組がアドレスリスト手段に存在する場合は、当該ノードは正規のノードであることが確認される。一方、ネットワーク層アドレスおよびデータリンク層アドレスの組がアドレスリスト手段に存在しなかった場合は、当該ノードは正規のノードではないことが確認される。

【0018】このようにして、セキュリティの優れたネットワーク運営が可能になる。第2の発明では、アドレス管理装置は、当該アドレス管理装置自身を要求元として、前記アドレス割り当て要求を疑似的に送出する。所

6

定の時間が経過する間に、疑似的に送出した前記アドレス割り当て要求に対する応答パケットが伝送されてきた場合、該応答パケットの送信元ノードのネットワーク層アドレスおよびデータリンク層アドレスを抽出する。

【0019】ところで、アドレス管理装置が1台だけしか存在しない場合は、応答パケットが伝送されてこないはずである。したがって、上記応答パケットに記述されたネットワーク層アドレスおよびデータリンク層アドレスを持つノードは、不正なアドレス管理装置であることが分かる。

【0020】このようにして、能動的に、ネットワークにおける不正なアドレス管理装置の存在を監視することができるので、不正なアドレス管理装置の早期発見を可能とし、セキュリティの優れたネットワーク運営が可能になる。

【0021】第3の発明では、既に割り当られたネットワーク層アドレスと対応するデータリンク層アドレスを組にしてアドレスリスト記憶手段に記憶している。アドレス管理装置は、当該アドレス管理装置自身を要求元として、前記アドレス割り当て要求を疑似的に送出する。所定の時間が経過する間に、疑似的に送出した前記アドレス割り当て要求に対する応答パケットが伝送されてきた場合、該応答パケットの送信元ノードのネットワーク層アドレスおよびデータリンク層アドレスを抽出する。抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組は、アドレスリスト手段に記憶された組の中に存在するか否かを判定される。

【0022】ネットワーク層アドレスおよびデータリンク層アドレスの組がアドレスリスト手段に存在する場合は、当該ノードは正規のアドレス管理装置であることが確認される。

【0023】一方、ネットワーク層アドレスおよびデータリンク層アドレスの組がアドレスリスト手段に存在しなかった場合は、当該ノードは正規のアドレス管理装置ではないことが確認される。

【0024】このようにして、能動的に、ネットワークにおける不正なアドレス管理装置の存在を監視することができるので、不正なアドレス管理装置の早期発見を可能とし、セキュリティの優れたネットワーク運営が可能になる。

【0025】第4の発明では、既に割り当られたネットワーク層アドレスと対応するデータリンク層アドレスを組にしてアドレスリストに登録する。アドレス管理装置は、ネットワーク上を伝送されるパケットをその宛先にかかわらず受信し、受信したパケットから、該パケットの発信元ノードのネットワーク層アドレスおよびデータリンク層アドレスの組または宛先ノードのネットワーク層アドレスおよびデータリンク層アドレスの組の少なくとも一方を抽出する。抽出されたネットワーク層アドレスおよびデータリンク層アドレスの組は、アドレスリス

トに登録された組の中に存在するかどうか判定される。

【0026】ネットワーク層アドレスおよびデータリンク層アドレスの組がアドレスリストに存在する場合は、当該ノードは正規のノードであることが確認される。一方、ネットワーク層アドレスおよびデータリンク層アドレスの組がアドレスリストに存在しなかった場合は、当該ノードは正規のノードではないことが確認される。

【0027】このようにして、セキュリティの優れたネットワーク運営が可能になる。第5の発明では、アドレス管理装置を同一管理範囲内に複数設置することで、それぞれが管轄するアドレス範囲を分担することにより、各アドレス管理装置の負荷を軽減することが可能となる。

【0028】その結果、アドレス管理システムの安定的な運用に寄与する。第6の発明によると、複数のアドレス管理装置とネットワーク全体のアドレスを管理するデータベースを用いて、各アドレス管理装置のシステムダウンへの迅速な対応が可能になる。その結果、アドレス管理システムの安定的な運用に寄与する。

【0029】

【実施例】以下、図面を参照しながら本発明の実施例を説明する。図1に、本実施例の基本システム構成を示す。図のように、本実施例では、ネットワーク2に、複数の端末装置（以下、一般ノードと呼ぶ）4と、本発明を適用した1台または複数台のアドレス管理装置6が接続される。

【0030】なお、以下では、一般ノードとアドレス管理装置とを区別しない場合があるので、便宜上、一般ノードとアドレス管理装置とを総称して、単に、「ノード」と呼ぶこととする。

【0031】ネットワーク2は、孤立して存在するものでも良い。あるいは、ネットワーク2はサブネットであり、他の1つまたは複数のサブネットと相互に接続されて、全体として1つのネットワークを構成するようなものであっても良い。言い換えると、ネットワーク内でブロードキャストの届く範囲を、サブネットつまりネットワーク2とする。この場合には、各サブネットは、網間接続装置により接続される。なお、あるサブネットには、アドレス管理装置6を設ける代わりに、他のサブネットに存在するアドレス管理装置6にパケットを転送する能力のあるアドレス管理中継装置を設ける場合もある。ネットワーク2がサブネットである場合には、あるサブネットに接続される一般ノード4が1台の場合もあり得る。

【0032】ネットワーク2としては、ブロードキャスト型LAN、例えばイーサネットを利用することができる。上記の他にも、本発明は、様々な形態のネットワークに適用することができる。

【0033】ところで、国際標準化機構ISO (International Organization for

Standardization) の開放型システム間相互接続参照モデル (Referenced Model of Open System Interconnection) では、通信のプロトコルを物理層、データリンク層、ネットワーク層、トランスポート層、セッション層、プレゼンテーション層、アプリケーション層の7つに分類している。

【0034】ネットワーク層は、ネットワークを通しての転送の基本単位を定義し、経路制御などを扱う層であり、ネットワーク層における転送や経路制御の際に用いるアドレスが、ネットワーク層アドレスである。

【0035】データリンク層は、ネットワーク層の下位に位置し、ハードウェアに依存するデータリンク層アドレスを用いて、ネットワークを通してのパケットの転送を行う。

【0036】本実施例のアドレス管理装置6は、ネットワーク2に接続された各一般ノード4から上記データリンク層アドレスに基づくアドレス割り当て要求があると、これに回答して該要求元の一般ノード4がパケット通信に用いる上記ネットワーク層アドレスを割り当てるものである。なお、各ノードのデータリンク層アドレスは、グローバルユニークである。

【0037】以下、アドレス管理装置のいくつかの例を詳細に説明する。

（第1の実施例）図2に、第1の実施例のアドレス管理装置の内部構成を示す。図に示すように、本実施例のアドレス管理装置は、通信プロトコル制御部11、アドレスリスト部13、アドレス/パラメータ割当制御部12、メッセージ制御部14、ネットワーク監視部15を用いて構成される。

【0038】通信プロトコル制御部11は、通信プロトコルに関する制御を行うものであり、例えばインターネットで使用されているネットワークを通じた通信のためのプロトコルであるTCP/IPに関する制御を行う。もちろん、通信プロトコル制御部11は、TCP/IP以外の他の通信プロトコルに対応するものであっても構わない。

【0039】次に、アドレスリスト部13に設けるアドレスリストについて説明する。図3に示すように、アドレスリスト部13は、ネットワーク層アドレスとデータリンク層アドレスの対応を登録するためのものである。本実施例では、ネットワーク層アドレスとして、その一種であるIPアドレスを、ネットワーク層アドレスとして、その一種であるMACアドレスを用いることとする。

【0040】最も一般的なアドレスリストとしては、図3のように、IPアドレスとMACアドレスを1対1に対応付けて登録するものである。この場合、IPアドレスがIP1であるノードのMACアドレスはMAC1であることを示しているとともに、MACアドレスがMA

C1であるノードのIPアドレスはIP1であることを示している。

【0041】1対1対応のアドレスリストにおいて、図4に示すように、IPアドレスに対応するMACアドレスがない場合がある。これは、現在そのIPアドレスに対応するノードが存在しないことを示している。例えば、アドレス割り当て前のアドレスリストの初期状態は、この状態である。

【0042】この他に、以下に示すようなアドレスリストが考えられる。1つめは、図5に示すように、1つのIPアドレスに対して複数のMACアドレスが対応する場合である。このようにすれば、例えばノードのイーザーメンテナン스가可能になる。アドレスリストには、実際に用いるノードのMACアドレスであるMAC1のみでなく、そのノードが何らかの理由により壊れて使用できなくなった場合に代わりに用いるバックアップ用のノードのMACアドレスであるMAC2やMAC3を登録しておく。そうすれば、MAC1のノードが故障した場合に、新しくMAC2のノードと交換した場合であっても、アドレスリストに登録されたノードとして認識され、イーザーメンテナン스가達成される。

【0043】2つめは、図6に示すように、1つのMACアドレスに対して複数のIPアドレスが対応する場合である。このようにすれば、例えばノード（特に一般ノード）の移動に対応することができる。あらかじめアドレスリストに、MACアドレスであるMAC1を持つノードを使用する可能性のある各ネットワークで有効なIPアドレスであるIP1とIP2を登録しておく。当初、IP1を割り当てられていたノードが移動をし、移動先で新たにIP2を割り当てられた場合には、移動前と移動後のノードの同一性が容易に確認できる。

【0044】3つめは、図7に示すように、IPアドレスとMACアドレスが多対多対応をする場合である。このような登録をあらかじめ行っておくと、イーザーメンテナンส์およびノードの移動への対応いづれも可能である。

【0045】次に、アドレスリスト部13について説明する。アドレスリスト部13は、上記のようなアドレスリストを備えている。本実施例では、アドレスリストは、アドレス管理装置のアドレスリスト131と、一般ノードのアドレスリスト132に分けて設けることとする。

【0046】アドレスリスト131は、アドレス管理装置のネットワーク層アドレスとデータリンク層アドレスを対応付けて登録する領域である。本実施例では、アドレスリスト131として、図8に示すように、IPアドレスとMACアドレスが1対1対応のアドレスリストを用いることにする。

【0047】本実施例では、アドレスリスト131を保持しているアドレス管理装置から見て、アドレスリスト

131に登録されているアドレス管理装置は正規のアドレス管理装置とみなし、一方、未登録のアドレス管理装置は不正なアドレス管理装置とみなす。そのために、アドレス管理装置をネットワークに接続して使用する際には、周辺の既に存在するアドレス管理装置の中で正規のアドレス管理装置と認識する必要のあるアドレス管理装置について、アドレス管理装置の使用前にあらかじめアドレスリスト131に登録しておく。ここでいう周辺とは、最も狭い範囲を考えた場合は同一管理範囲内を指すこととなり、それ以上範囲が広くても差し支えない。後からアドレス管理装置が周辺のネットワークに付加された場合にも、そのアドレス管理装置を正規のアドレス管理装置として認識する必要のあるときは、アドレスリスト131への登録を行う。

【0048】後述するような方法で、ネットワーク監視部14がアドレスリスト131を参照することにより、アドレスリスト131に未登録のアドレス管理装置から送出されたパケットの到来を発見すると、不正なアドレス管理装置が存在すると判断し、その旨を他のノードやネットワークシステム管理者等に報告することができる。不正なアドレス管理装置が発生する原因としては、登録誤りや侵入等が挙げられる。

【0049】一方、アドレスリスト132は、アドレス管理装置が一般ノードからの割り当て要求に応じてアドレスを割り当てるために所持しているネットワーク層アドレス、およびアドレス管理装置が一般ノードからの割り当て要求に応じてアドレスを割り当てたネットワーク層アドレスとそれに対応するデータリンク層アドレスを保持するものである。図9に、本実施例で用いる一般ノードのアドレスリスト132の一例を示す。図のように、アドレス管理装置が一般ノードの割り当て要求に応じてアドレスを割り当てるために所持しているネットワーク層アドレスに関しては、そのネットワーク層アドレスが割り当て可能な状態にある場合にはunlock状態、そうでない場合にはlock状態とし、その状態を明示する。既にデータリンク層アドレスに対応するよう割り当てられているネットワーク層アドレスは、lock状態、unlock状態いづれでもない第3の状態とする。

【0050】lock状態は、例えば次のような場合に発生する。一度使用されたネットワーク層アドレスは、以前に使用していた一般ノードからこのネットワーク層アドレスが返却されても、直ぐに使用可能とせず、返却されてから規定された時間が経過するまで再利用できないものとする場合で、この規定時間内、ネットワーク層アドレスはlock状態となる。lock状態にあるネットワーク層アドレスは、他の一般ノードへの割り当てはできない。

【0051】unlock状態は、今まで一度も使用されていない未使用のネットワーク層アドレスであるか、

11

あるいは使用された後に返却され既にlock状態を解除されたネットワーク層アドレスであり、他の一般ノードによる再利用が可能である。

【0052】このアドレスリスト132を保持しているアドレス管理装置から見て、アドレスリスト132に登録されている一般ノードは正規の一般ノードであり、未登録の一般ノードは不正な一般ノードとみなす。

【0053】後述するような方法で、ネットワーク監視部14がアドレスリスト132を参照することにより、アドレスリスト132に未登録のノードから送出された10 パケットの到来を発見すると、不正な一般ノードが存在すると判断し、その旨を他のノードやネットワークシステム管理者等に報告することができる。

【0054】アドレス管理装置は、ネットワークに接続した一般ノードからのアドレス割り当て要求に応じてネットワーク層アドレスの付与および登録手続きを行うため、あらかじめネットワーク層アドレスを保持している。本実施例では、アドレスリスト部13があらかじめ保持しているIPアドレスは、当該アドレス管理装置が20 管轄するネットワークのネットワーク識別子を持つ全てのIPアドレスである。

【0055】IPアドレスの保持方法には、例えば以下に示すように、種々の形態が考えられ、状況に応じて適宜設定すれば良い。例えば、アドレス管理装置の台数／配置や用途に応じ、アドレス管理装置が管轄するネットワークのネットワーク識別子をもつすべてのIPアドレスを保持する方法、アドレス管理装置が管轄するネットワークのネットワーク識別子をもつIPアドレスのうち一部を保持する方法、アドレス管理装置が管轄するネットワークのネットワーク識別子以外のネットワーク識別子をもつIPアドレスを保持する方法、アドレス管理装置が管轄するネットワークのネットワーク識別子をもつIPアドレスの一部あるいは全部とアドレス管理装置が管轄するネットワークのネットワーク識別子以外のネットワーク識別子をもつIPアドレスを保持する方法などが考えられる。

【0056】なお、本実施例のアドレスリスト部13に登録するネットワーク層アドレスとデータリンク層アドレスの対応については、前述した4つの形態、すなわちネットワーク層アドレスとデータリンク層アドレスが1 40 対1に対応する形態、ネットワーク層アドレスひとつに対して複数のデータリンク層アドレスが対応する形態、データリンク層アドレスひとつに対して複数のネットワーク層アドレスが対応する形態、ネットワーク層アドレスとデータリンク層アドレスが多対多対応する形態のうちから、必要に応じて適宜選択すれば良い。

【0057】ところで、本実施例では、アドレスリスト部13に、アドレス管理装置のアドレスリスト131と、一般ノードのアドレスリスト132を分けて設けたが、アドレス管理装置と一般ノードを区別せずに1つの

12

アドレスリストとして設けることも可能である。この場合、後述するような方法で、ネットワーク監視部14がアドレスリストを参照することにより、アドレスリストに未登録のノードから送出されたパケットの到来を発見すると、不正なノードが存在すると判断し、その旨を他のノードやネットワークシステム管理者等に報告することができる。

【0058】次に、アドレス／パラメータ割り当て制御部12について説明する。アドレス／パラメータ割り当て制御部12は、ネットワーク層アドレスと必要なパラメータの割り当て制御を行うものであり、例えばIETFのRFC1541に定められた仕様と各アドレス管理装置毎のアドレスおよびパラメータ付与方針に従い、ノードからのアドレス割当要求に対応して、IPアドレスおよび各種パラメータ付与の手続きを行う。もちろん、アドレス／パラメータ割り当て制御部12は、IETFのRFC1541以外の、他の方式に基づいた制御を行うものであっても構わない。なお、上記パラメータとしては、例えば当該IPアドレスの有効期間を設定する場合における当該有効期間などがある。

【0059】次に、通信プロトコル制御部11について説明する。本実施例では、通信プロトコル制御部11は、例えばTCP/IPに代表されるような通信プロトコルの制御、すなわち通常のネットワークにおけるパケットの経路制御等を行う。アドレス管理に最も関係のある制御としては、通信プロトコルとしてTCP/IPを例にとると、TCP/IPプロトコル群の一つでデータリンク層のプロトコルであるARP(Address Resolution Protocol, RFC826)に関連してARPテーブルを備え、その時点でのネットワーク層アドレスとデータリンク層アドレスの対応を保持している。アドレス管理装置は、ネットワーク上を流れるARPメッセージに対してアドレスリスト部13を参照してARP応答メッセージを作成することはせず、全て通信プロトコル制御部11において対応する。

【0060】次に、ネットワーク監視部14について説明する。ネットワーク監視部14は、ネットワークを流れるパケットの監視を行うものである。図10に、本実施例のネットワーク監視部14の構成を示す。図のように、ネットワーク監視部14は、パケット判別部141とアドレス情報処理部142から構成される。

【0061】まず、ネットワーク監視部14は、物理的手段等により当該アドレス管理装置自身宛のパケットのみならずその他の宛先へのパケットをもネットワークから取り込む。

【0062】パケット判別部141は、取り込まれたパケットの内部の情報を見て、例えばDHCPメッセージのパケットを判別し、アドレス情報処理部142を経由せずに直接アドレス／パラメータ割当制御部12に渡したり、ARPメッセージのパケットを判別し、アドレス

情報処理部142を経由せずに直接通信プロトコル制御部11に渡す。他の様々なパケットに対しても、あらかじめパケット判別部141においてパケット判別手段と適切なパケットの送り先を指定しておくことにより、アドレス管理装置内部における当該パケットの判別が可能になる。例えば、ARPパケットは、パケット判別部141により通信プロトコル制御部11へ制御を渡すべきパケットと判断され、通信プロトコル制御部11へ渡される。また、例えば、DHCP Offerメッセージ (RFC1533) は、パケット判別部141によりアドレス情報処理部142へ制御を渡すべきパケットと判断され、アドレス情報処理部142へ渡される。

【0063】アドレス情報処理部142では、判別されたパケットの種類毎に夫々必要なアドレスをパケットの中から読み込み、アドレスリスト部13と比較参照し、例えば後述するに不正なノードが検出された場合など、必要があればメッセージ制御部15に対し任意の宛先へのメッセージの送出を依頼する。

【0064】次に、ネットワーク監視部14とアドレスリスト部13を用いて不正なノードを検知する検出方法について説明する。この検出方法の一例として、図11に、DHCP Offerメッセージを監視し、不正なアドレス管理装置が存在しないかどうかを判断する手順を示す。DHCP Offerメッセージとは、ノードからのアドレス要求を受けたアドレス管理装置が、提供できるアドレスや必要なパラメータをノードに提示するメッセージである。この手順は、以下の通りである。

【0065】まず、ネットワーク監視部14は、ネットワーク上を流れるパケットを取り込む(ステップS1)。次に、そのパケットがDHCP Offerメッセージのパケットであるかどうかを、UDP (User Datagram Protocol, RFC768) データフィールドに収納されたDHCPメッセージのOPフィールドを見て判断する(ステップS2)。そのパケットがDHCP Offerである場合には、そのDHCP Offerメッセージを送出したアドレス管理装置のネットワーク層アドレスを、DHCPメッセージのs i a d d rフィールドあるいはg i a d d rフィールドから読み出す(ステップS3)。読み出したアドレス管理装置のネットワーク層アドレスと、アドレス管理装置のアドレスリスト131に既に登録されているネットワーク層アドレスとを比較参照し、パケットを発信したアドレス管理装置が登録済のアドレス管理装置であるかを調べる(ステップS4)。パケットを発信したアドレス管理装置のネットワーク層アドレスが、アドレスリスト131に登録してあれば問題はない。パケットを発信したアドレス管理装置のネットワーク層アドレスがアドレスリスト131に登録されていない場合には、不正なアドレス管理装置がネットワーク内に存在するものと考えられるので、ネットワーク管理者にその旨報告する

等して対処する(ステップS5)。

【0066】本実施例では、DHCP Offerメッセージのパケット監視について述べたが、通常のパケット等、ネットワーク上を流れるその他のパケットについても、同様のパケット監視が可能であり、不正なアドレス管理装置だけでなく、アドレスリスト132を参照することにより、不正な一般のノードを検出することもできる。

【0067】また、パケットの送信元のアドレスだけでなく、パケットの宛先のアドレスを読むことによって、宛先ノードが不正であるか否かを判断することもできる。次に、以下では、本実施例のアドレス管理装置を用いて、アドレス割り当てに際してのセキュリティを確保する方法、すなわち不正な装置を検知するについて説明する。

【0068】ネットワークには、不正なアドレス管理装置が出現する可能性と、不正な一般ノードが出現する可能性がある。不正なアドレス管理装置や不正な一般ノードがネットワーク内に存在し、正規のアドレス管理装置や一般ノードの通信を妨げたり、盗聴をするようでは、そのネットワークで重要事項について通信を行うことは大変危険である。

【0069】そこで、不正なアドレス管理装置や不正な一般ノードがネットワーク内に存在しないように、また仮に不正なアドレス管理装置や不正な一般ノードが存在した場合には即座に検出し取り除く手をしなければならぬ。

【0070】その方法について、(i) 不正なアドレス管理装置がネットワークに存在する場合の正規のアドレス管理装置の対応、(ii) 不正なアドレス管理装置がネットワークに存在する場合の正規の一般ノードの対応、(iii) 不正なアドレス管理装置がネットワークに存在する場合の正規のアドレス管理装置と一般ノードの対応、(iv) 不正な一般ノードがネットワークに存在する場合の正規のアドレス管理装置の対応、(v) 不正な一般ノードがネットワークに存在する場合の正規の一般ノードの対応、に分けて以下に述べる。

【0071】(i) 不正なアドレス管理装置がネットワークに存在する場合の正規のアドレス管理装置の対応
不正なアドレス管理装置がネットワークに存在する場合、正規のアドレス管理装置の対応としては、(a) 正規のアドレス管理装置がネットワークを流れるパケットの監視を行う方法がある。

【0072】この方法としては、前述したようにネットワーク監視部14とアドレスリスト部13を用いてネットワーク上を流れるパケットを監視する方法がある。また、上記aの方法の他には、(b) 正規のアドレス管理装置が定期的に疑似アドレス割り当て要求を送出して周囲の反応をうかがい、応答してきたアドレス管理装置が不正なアドレス管理装置でないかどうかアドレスリスト

部13を用いて調べるような方法がある。この方法については、第2の実施例として後で詳細に説明する。なお、第1の実施例または第2の実施例のアドレス管理装置を正規のアドレス管理装置として複数設置し互いに監視を行う方法を第3の実施例および第4の実施例として後で詳細に説明する。

【0073】(ii) 不正なアドレス管理装置がネットワークに存在する場合の正規の一般ノードの対応

ここでは、不正なアドレス管理装置がネットワークに存在する場合の正規の一般ノードの対応について説明する。アドレス管理装置からIPアドレスを割り当てられた一般ノードは、その割り当てられたIPアドレスを用いて通信をはじめる前に、そのIPアドレスを使用しているノードが既にネットワーク内に存在するか否か、ARP(Address Resolution Protocol)を行って調べることができる。ARPは、IPアドレスに対応するMACアドレスを尋ねるプロトコルである。ARPのメッセージに記載されたIPアドレスを割り当てられているノードは、ARPに対する応答メッセージで、当該IPアドレスに対応するMACアドレスをARPメッセージを送出したノードに知らせる。IPアドレスの割当てが適切に行われ、アドレスリスト部13にも記載されている場合には、この新たに割り当てられたIPアドレスに対応するMACアドレスを尋ねるARPに対する応答はないはずである。割り当てられたIPアドレスが何らかの理由により既に他のノードに割り当てられていた場合等には、ARPに対する応答がある。ARPへの応答があった場合は、一般ノードはシステム管理者あるいはアドレス管理装置等にその旨報告するとともに、新たなIPアドレスの割り当てを要求して対処することができる。

【0074】(iii) 不正なアドレス管理装置がネットワークに存在する場合の正規のアドレス管理装置と一般ノードの対応 (共通部分)

アドレス要求を行った一般ノードに割り当てられたIPアドレスが、他のノードに既に割り当てられているIPアドレスではないが、正規のアドレス管理装置がアドレス要求を行った一般ノードに対して付与したIPアドレスではないことを、正規のアドレス管理装置が前述したようなネットワーク監視部14とアドレスリスト部13を用いてネットワーク上を流れるパケットを監視する方法により発見した場合は、次のようにして対処する。

【0075】正規のアドレス管理装置は、不正なアドレス管理装置から一般ノードに勝手に付与されたIPアドレスが、当該一般ノードに使用されることを阻止するため、アドレスリスト部13に不正なアドレス管理装置から勝手に当該一般ノードに付与されたIPアドレスと同一のIPアドレスが存在する場合は、そのIPアドレスが他の一般ノードに割り当てられることのないようlock状態にする等して対策を施す。

【0076】その後、不正なアドレス管理装置からIPアドレスを付与されたノードが、付与されたIPアドレスの正当性を確認するためにARPメッセージを送信した場合、このメッセージに対して正規のアドレス管理装置は、疑似的にARP応答メッセージを出す。この疑似的に出されたARP応答メッセージ内の、IPアドレスに対応するMACアドレスを示す部分には、当該正規のアドレス管理装置のMACアドレスを記しておけばよい。このARP応答メッセージにより、アドレス要求を行った一般ノードは、当初(不正なアドレス管理装置から)付与されたIPアドレスの使用は適切ではないと判断し、新たにIPアドレスの要求を行うことができる。

【0077】正規のアドレス管理装置は、登録されていないにも関わらず一般ノードにアドレスを割り当てようとしたアドレス管理装置が存在する旨をシステム管理者に報告する等した後、適宜そのIPアドレスのlock状態を解除する等して対処することができる。

【0078】(iv) 不正な一般ノードがネットワークに存在する場合のアドレス管理装置の対応

ここでは、不正な一般ノードがネットワークに存在する場合のアドレス管理装置の対応について説明する。アドレス管理装置は、ネットワーク監視部14とアドレスリスト部13を用いてネットワーク上を流れるパケットを監視する。アドレス管理装置では、ネットワーク監視部14からパケットを取り込み、パケット判別部141にてパケットの転送先を判断し、アドレス情報処理部142以外に転送されることが規定されたパケットを除き、アドレス情報処理部142に転送する。アドレス情報処理部142にて、パケットのヘッダ部からMACアドレスとIPアドレスを読み出し、アドレスリスト部13にパケットから読みだしたIPアドレスとMACアドレスの対と同一の対が登録されているかどうか照合する。アドレスリストに既に登録されている一般ノードであることが確認されたものは、正規の一般ノードであり、登録されていなかった場合は不正な一般ノードであることがわかる。未登録の不正なアドレスであった場合には、システム管理者に報告する等して対処することができる。

【0079】(v) 不正な一般ノードがネットワークに存在する場合の正規の一般ノードの対応

ここでは、不正な一般ノードがネットワークに存在する場合に、正規の一般ノードの対応について説明する。一般ノードは、IPアドレス設定時、更新時、または一定時間毎などにARPを行う。ARPに対する応答がなければ、そのIPアドレスを使用しているノードは存在せず、使用しても差し支えないものと考えられる。一方、ARPに対する応答があった場合、応答があるということは、そのIPアドレスをその時点で使用しているノードが存在することを示しているの、そのIPアドレスの使用は不適切であることが判明する。ARPによって、不適切なアドレス割り当てに気付いた一般ノード

は、そのIPアドレスの使用を控え、新規のIPアドレスの割り当てを要求することで、対処することができる。また、IPアドレスが重複している旨などをシステム管理者あるいはアドレス管理装置等に報告するなどして対応することができる。

【0080】ところで、前述したように、メッセージ制御部15は、ネットワーク監視により送出する必要性の生じたメッセージを任意の宛先に送出する制御を行う。本実施例のアドレス管理装置が複数ある場合、各アドレス管理装置のメッセージ制御部15から送出されるメッ
10 セッセージを集中的に受信し管理する監視装置をネットワーク内のいずれかの場所に設けても良い。この点は、後述する各実施例についても同様である。

【0081】(第2の実施例) 第1の実施例では、ネットワークを流れるパケットを監視して不正なノードを検知する受動的な検出方法を詳細に説明したが、本実施例では、アドレス管理装置が特別のメッセージを送出することにより、登録されていない不正なアドレス管理装置の存在を明らかにする能動的な検出方法を説明する。

【0082】本実施例のアドレス管理装置は、図12に示すように、基本的には第1の実施例のアドレス管理装置と同様の構成を有しており、これにセキュリティ保守部20を付加したものである。

【0083】本実施例のアドレス管理装置では、第2の実施例の機能に加え、セキュリティ保守部20を用いてネットワークに擬似的にアドレス割り当て要求を送出し、応答してきたアドレス管理装置が不正なアドレス管理装置でないかどうかアドレスリスト部13を用いて調べる機能を有する。この操作は、例えば定期的に行われる。

【0084】図13に、不正なアドレス管理装置を能動的に検出するための手順を示す。まず、アドレス管理装置は、登録されていない不正なアドレス管理装置を検出するため、通常は一般ノードが送出するアドレス割り当て要求と同じ仕様のアドレス割り当て要求を擬似的に送出する(ステップS11)。

【0085】アドレス割り当て要求としては、例えばDHCPメッセージを利用することができる。図14に、DHCPメッセージのパケットフォーマットを示す。DHCPメッセージのアドレス要求を示す場合には、OP
40 フィールドにアドレス要求のコードを書き込む。アドレス割り当て要求のトランザクションIDを示すフィールドに適当な番号を入れ、そのトランザクションIDにより、自分の送出した擬似アドレス割り当て要求を他のパケットから区別する。この際、擬似的なアドレス割り当て要求に自分のMACアドレスを含めても差し支えない。

【0086】アドレス管理装置から送出された擬似的なアドレス割り当て要求は、サブネットにブロードキャストされる。ブロードキャストにより自分自身にもどって
50

きた当該擬似的なアドレス割り当て要求は、パケットに含まれるトランザクションIDで自己が送出したアドレス割り当て要求であることが判明するので無視する。

【0087】さて、そのローカルネットワークには、元々、アドレス管理装置が当該アドレス割り当て要求を出したアドレス管理装置1台だけしか存在しない場合は、応答はないはずである。また、ローカルネットワークに、複数台のアドレス管理装置が存在する場合は、他のアドレス管理装置から応答があつてしかるべきである。しかし、ここでは、ネットワークに存在するアドレス管理装置の台数にかかわらず、以下の処理を続ける。

【0088】ネットワーク上を流れるパケットを監視するうちに(ステップS12)、擬似アドレス割り当て要求に対してアドレス提案を内容とする応答があつた場合は(ステップS13)、その応答パケットのsiaddrフィールドに含まれる応答したアドレス管理装置のIPアドレスを見る。

【0089】応答したアドレス管理装置のIPアドレスが擬似アドレス割り当て要求を送出したアドレス管理装置のアドレスリストに登録された正当なアドレス管理装置のものである場合は(ステップS14)、不正なアドレス管理装置は存在しないものと推定される。そのため、特にシステム管理者に通知するなどの必要性はない。登録された正規のアドレス管理装置からの擬似的アドレス割り当て要求に対するアドレス提案を内容とする応答に対しては、明示的にアドレス不要の通知を行う。そのアドレス管理装置が、一定の時間以上アドレス割り当て要求に対するアドレス提案を内容とする応答に対するノードの応答がない場合はアドレス提案を無効にするというタイムアウト制を導入している場合は、そのまま何もせずに放置しても構わない。

【0090】一方、応答を送出したアドレス管理装置のアドレスが擬似アドレス割り当て要求を送出したアドレス管理装置のアドレスリストに登録された正当なアドレス管理装置のものでなかった場合は(ステップS14)、その事実を発見したアドレス管理装置がシステム管理者に警告パケットを送信する等して対処する(ステップS15)。

【0091】ところで、前述のようにアドレス管理装置が当該アドレス割り当て要求を出したアドレス管理装置1台だけしか存在しない場合は、応答はないはずである。そこで、正規のアドレス管理装置が1台しかない場合は、アドレスリストを参照せずに、応答があつたことをもって、不正なアドレス管理装置が存在するものとみなすようにしても良い。

【0092】(第3の実施例) ここでは、1つのネットワーク内に、第1の実施例または第2の実施例アドレス管理装置を複数台設置し、アドレス管理の効率化と通信のセキュリティの向上を図った例について説明する。

【0093】本実施例では、1つのネットワーク内に設

19

けた複数のアドレス管理装置々は、管理すべきアドレスを分担し、互いに異なる範囲のアドレスに関する管理を受け持つようにしている。例えば、図15に示す通り、1つのサブネット2内に2台のアドレス管理装置6-A、6-Bを設置し、夫々が管轄するアドレスの範囲を、例えばアドレス管理装置6-AについてはIP0～IP19、アドレス管理装置6-BについてはIP20～IP39とする。当然のことながら、図15のアドレス管理装置6-A内のアドレスリストA（図示せず）に保持されているIPアドレスと、アドレス管理装置6-B内のアドレスリストB（図示せず）に保持されているIPアドレスには、重複するものはない。この方法によると、1台のアドレス管理装置が管理すべきアドレスの数を少なくすることができ、アドレス管理の負担を小さくすることができる。

【0094】一般ノードについては、その一般ノードが正規の一般ノードであるか不正な一般ノードであるかは、アドレス管理装置間で何ら情報交換を行わない場合には、アドレス管理装置夫々が所有するアドレスリストの範囲のみでしか判断できない。そこで、アドレス管理装置がネットワーク監視においてアドレスリスト部13に登録されていない一般ノードを発見した場合に、同じネットワークを担当する他のアドレス管理装置に対し、IPアドレスとMACアドレスの対を提示して、問い合わせ先のアドレス管理装置のアドレスリストにそのアドレス対が登録されているかを探ねることも可能である。同じネットワークを担当する全てのアドレス管理装置からの問い合わせに対する応答を受けたあと、いずれのアドレス管理装置のアドレスリストにも登録されていないことが明らかとなった場合には、他のノードやシステム管理者に警告パケットを送信する等して対処することができる。

【0095】（第4の実施例）ここでは、ひとつのネットワーク内に、第1の実施例または第2の実施例のアドレス管理装置を複数台設置し、アドレス管理の効率化と通信のセキュリティの向上を図る例について説明する。本実施例は、第3の実施例とは異なり夫々のアドレス管理装置が管理するアドレスの範囲を分担することはせず、図16に示す通り、アドレスを管理する共通アドレスリスト・データベース（以下、データベース）30における情報を共有し、ノードからのアドレス割り当て要求があった場合、各アドレス管理装置6-C、6-Dは、必要に応じてそのデータベース30を参照し、互いに冗長系として機能させる方法である。

【0096】まず、サブネット毎、いくつかのサブネット・グループ毎、またはネットワーク全体に1つ、そのサブネット内、サブネット・グループ内、またはネットワーク内の端末に付与可能なアドレスを記載したアドレスリストを保持するデータベース30を設置する。

【0097】アドレス管理装置は、ノードからアドレス

20

要求が届いた際あるいはパケット監視を行う際、その他アドレス管理情報を必要とする場合に、データベース30にアドレスの最新情報の問い合わせを行う。データベース30は、アドレス管理装置からの問い合わせに応じてアドレスの最新情報を提供する。アドレス管理装置は、データベース30から提供されたアドレスの最新情報を基に、アドレスおよび必要なパラメータを一般ノードに割り当てる制御を行う。

【0098】一般ノードからアドレス管理装置へのアドレスやパラメータの付与要求に対して、要求があつてから実際に要求を受信したアドレス管理装置がその要求に対応する処理を開始するまでの反応時間およびアドレス管理装置がどのような方針でアドレスおよびパラメータを与えるかは、個々のアドレス管理装置において自由に設定でき、同じデータベース30にアクセスするアドレス管理装置間で処理開始までの時間とアドレスおよびパラメータ付与方針を統一する必要はない。特に、上記反応時間を、各アドレス管理装置について、互いに異なる長さに設定すると、例えば最初に動作したアドレス管理装置のアドレス割り当てが成功に完了した場合、他のアドレス管理装置は、ネットワークにアドレス割り当て処理のためのパケットを送出する必要がなくなり、あるいはアドレス割り当て処理自体を行う必要がなくなるので、ネットワーク資源利用の効率化や処理の効率化を図ることができる。

【0099】パケットの正当性を判断するネットワーク監視を行う際には、同一サブネットなど同じ範囲を担当するアドレス管理装置間で、ネットワーク層アドレスの最下位ビットの奇数の場合はあるアドレス管理装置が監視をし、偶数の場合はもうひとつのアドレス管理装置が監視をするなど、実際にアドレス管理装置からデータベース30までアドレスリストとの照合を行う仕事を分担してもよい。

【0100】一方、このように複数のアドレス管理装置とデータベースからなる構成の場合、アドレス管理装置が互いに冗長系として機能し得る。もし仮にアドレス管理装置の内1台がシステムダウンしたとしても、一般ノードからのアドレスおよびパラメータ割り当て要求は、システムダウンしたアドレス管理装置とは異なるアドレスおよびパラメータの割り当て要求を受信してから処理を開始するまでの時間を持つ他のアドレス管理装置により処理されるか、あるいはDHCPのアドレスおよびパラメータ割り当て要求を再送する機能により処理される。

【0101】アドレス管理装置がシステムダウンしているか否かを判断する手段としては、第2の実施例に説明した方法を応用することが可能である。つまり、同じ管理範囲内に存在するアドレス管理装置がシステムダウンを起こしていないかどうか、アドレス管理装置あるいはアドレス管理装置と同等の機能をもつデータベースが、疑似的にアドレス割り当て要求を送出し、その応答

21

の有無を確認することができる。また、本発明は、上述した各実施例に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【0102】

【発明の効果】本発明によると、正規のネットワーク層アドレスとデータリンク層アドレスの組を記憶しておき、ネットワーク上を伝送されるパケットに記述されたネットワーク層アドレスおよびデータリンク層アドレスが記憶されたものであるか照合することにより、不正な

アドレス管理装置および不正な端末装置の存在を監視することができる。

【0103】第2の発明では、唯一存在するアドレス管理装置は、当該アドレス管理装置自身を要求元としてアドレス割り当て要求を疑似的に送出し、所定の時間が経過する間に応答パケットが伝送されてきた場合、その事実を持って不正なアドレス管理装置の存在を知ることができる。

【0104】このようにして、能動的に、ネットワークにおける不正なアドレス管理装置の存在を監視することができるので、不正なアドレス管理装置の早期発見が可能になる。

【0105】第3の発明では、正規のネットワーク層アドレスとデータリンク層アドレスの組を記憶しておき、アドレス管理装置は、当該アドレス管理装置自身を要求元としてアドレス割り当て要求を疑似的に送出し、所定の時間が経過する間に応答パケットが伝送されてきた場合、応答パケットに記述されたネットワーク層アドレスおよびデータリンク層アドレスが記憶されたものであるか照合することにより、不正なアドレス管理装置の存在を監視することができる。

【0106】このようにして、能動的に、ネットワークにおける不正なアドレス管理装置の存在を監視することができるので、不正なアドレス管理装置の早期発見が可能になる。

【0107】第4の発明では、正規のネットワーク層アドレスとデータリンク層アドレスの組を記憶しておき、ネットワーク上を伝送されるパケットに記述されたネットワーク層アドレスおよびデータリンク層アドレスが記

22

憶されたものであるか照合することにより、不正なアドレス管理装置および不正な端末装置の存在を監視することができる。

【図面の簡単な説明】

【図1】本発明を適用するネットワーク構成の一例を示す図

【図2】本発明の第1の実施例に係るアドレス管理装置の内部構成を示す図

【図3】同実施例のアドレスリストの一例を示す図

【図4】IPアドレスに対応するMACアドレスが存在しない場合のアドレスリストを示す図

【図5】アドレスリストの他の例を示す図

【図6】アドレスリストのさらに他の例を示す図

【図7】アドレスリストのさらに他の例を示す図

【図8】アドレス管理装置のアドレスリストを示す図

【図9】一般ノードのアドレスリストを示す図

【図10】ネットワーク監視部の内部構成を示す図

【図11】同実施例におけるパケットを監視する動作の一例を示すフローチャート図

【図12】本発明の第2の実施例に係るアドレス管理装置の内部構成を示す図

【図13】同実施例における不正なアドレス管理装置を監視する動作の一例を示すフローチャート図

【図14】DHCPメッセージフォーマットを示す図

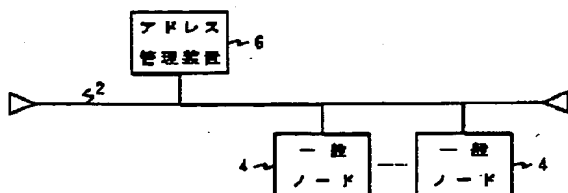
【図15】本発明の第3の実施例のシステム構成を示す図

【図16】本発明の第4の実施例のシステム構成を示す図

【符号の説明】

2…ネットワーク、4…一般ノード、6、6-A、6-B、6-C、6-D…アドレス管理装置、11…通信プロトコル制御部、12…アドレス/パラメータ割当制御部、13…アドレスリスト部、131…アドレスリスト、132…アドレスリスト、14…ネットワーク監視部、141…パケット判別部、142…アドレス情報処理部、15…メッセージ制御部、20…セキュリティ保守部、30…共通アドレスリストデータベース

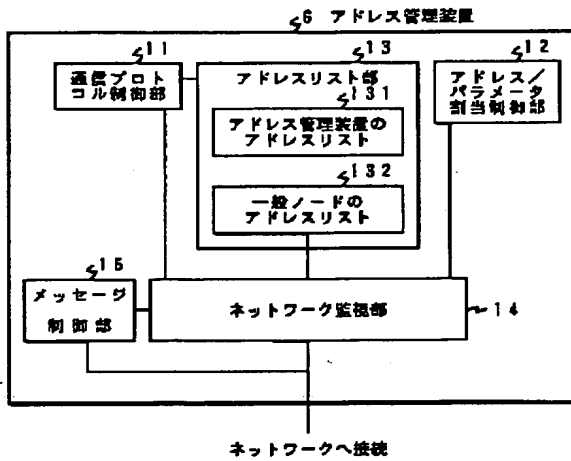
【図1】



【図3】

IPアドレス	MACアドレス
IP1	MAC1
IP2	MAC2
⋮	⋮

【図2】



【図5】

IPアドレス	MACアドレス (複数可)			
IP1	MAC1	MAC2	MAC3	...
IP2	MAC5	MAC6	MAC7	MAC8
⋮	⋮	⋮	⋮	⋮

【図7】

IPアドレス (複数可)			MACアドレス (複数可)		
IP1	IP2	IP3	MAC1	MAC2	MAC3
IP5	IP7	...	MAC10	MAC12	MAC13
⋮	⋮	⋮	⋮	⋮	⋮

【図9】

lock状態	IPアドレス (複数可)		MACアドレス (複数可)	
unlock	IP1
...	IP2	IP3	MAC1	...
...	IP4	...	MAC2	MAC3
...	IP5	IP6	MAC4	MAC5
...	IP7	...	MAC6	...
lock	IP8

【図4】

IPアドレス	MACアドレス
IP1	...
IP2	...
⋮	⋮

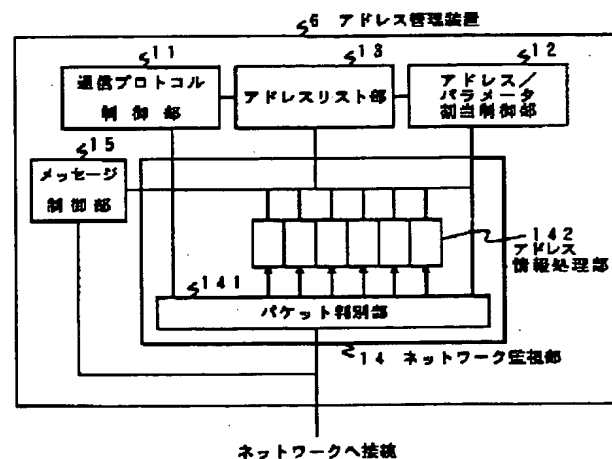
【図6】

IPアドレス (複数可)				MACアドレス
IP1	IP2	MAC1
IP3	IP4	IP5	...	MAC2
⋮	⋮	⋮	⋮	⋮

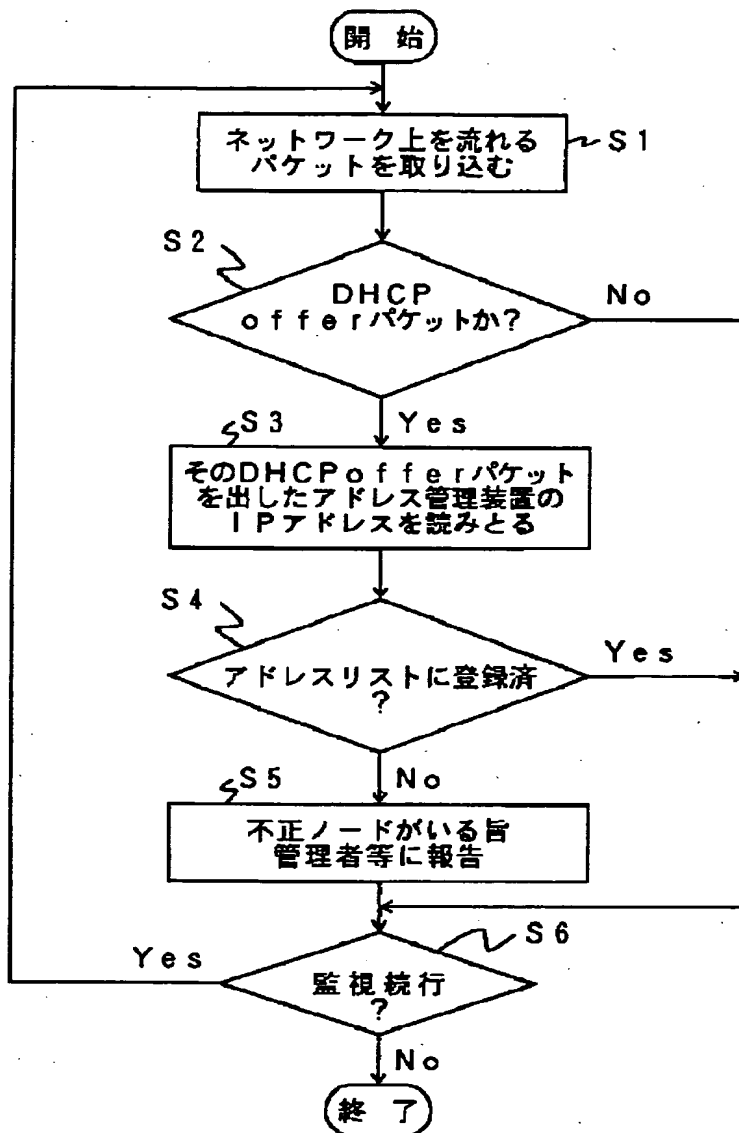
【図8】

IPアドレス	MACアドレス
IP1	MAC1
IP2	MAC2
⋮	⋮

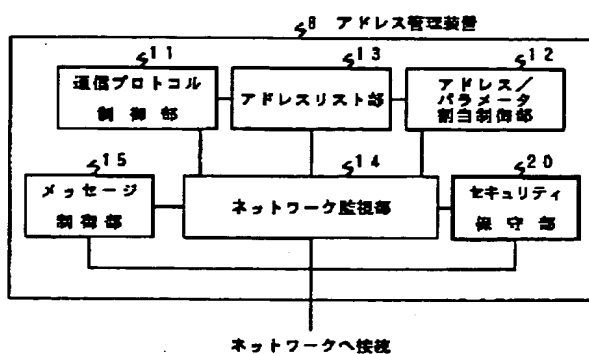
【図10】



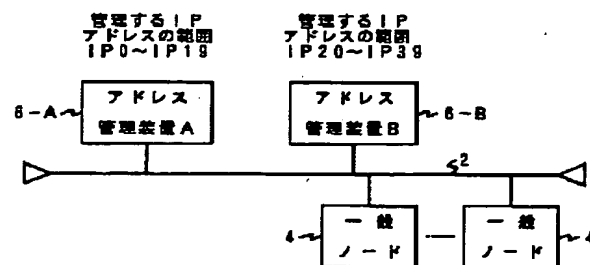
【図11】



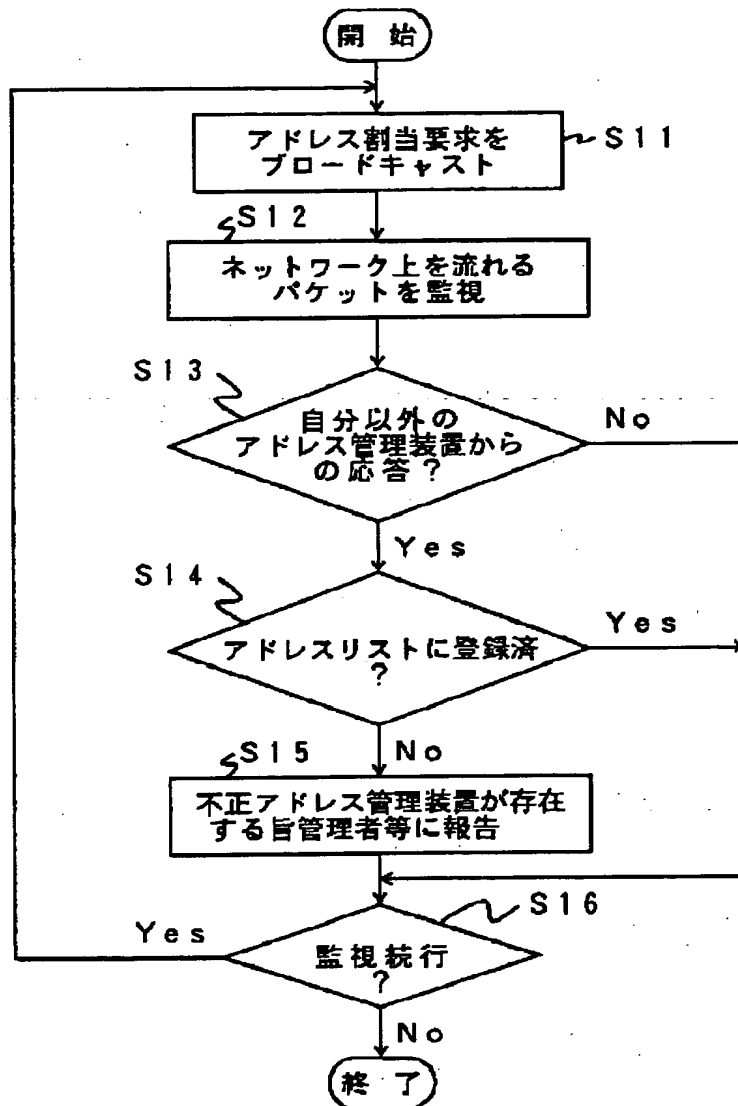
【図12】



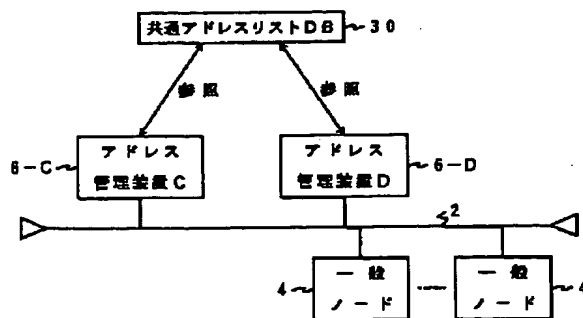
【図15】



【図13】



【図16】



【図14】

0	8	16	24
OP (1)	h type (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options (312)			

DialogIP

DEVICE AND METHOD FOR ADDRESS MANAGEMENT (08-186569
Publication Number: JP 8186569 A) , July 16, 1996

Inventors:

- AMI JUNKO
- OKAMOTO TOSHIO

Applicants

- TOSHIBA CORP (A Japanese Company or Corporation), JP (Japan)

Application Number: 06-326436 (JP 94326436) , December 27, 1994

International Class (IPC Edition 6):

- H04L-012/28
- G06F-013/00

JAPIO Class:

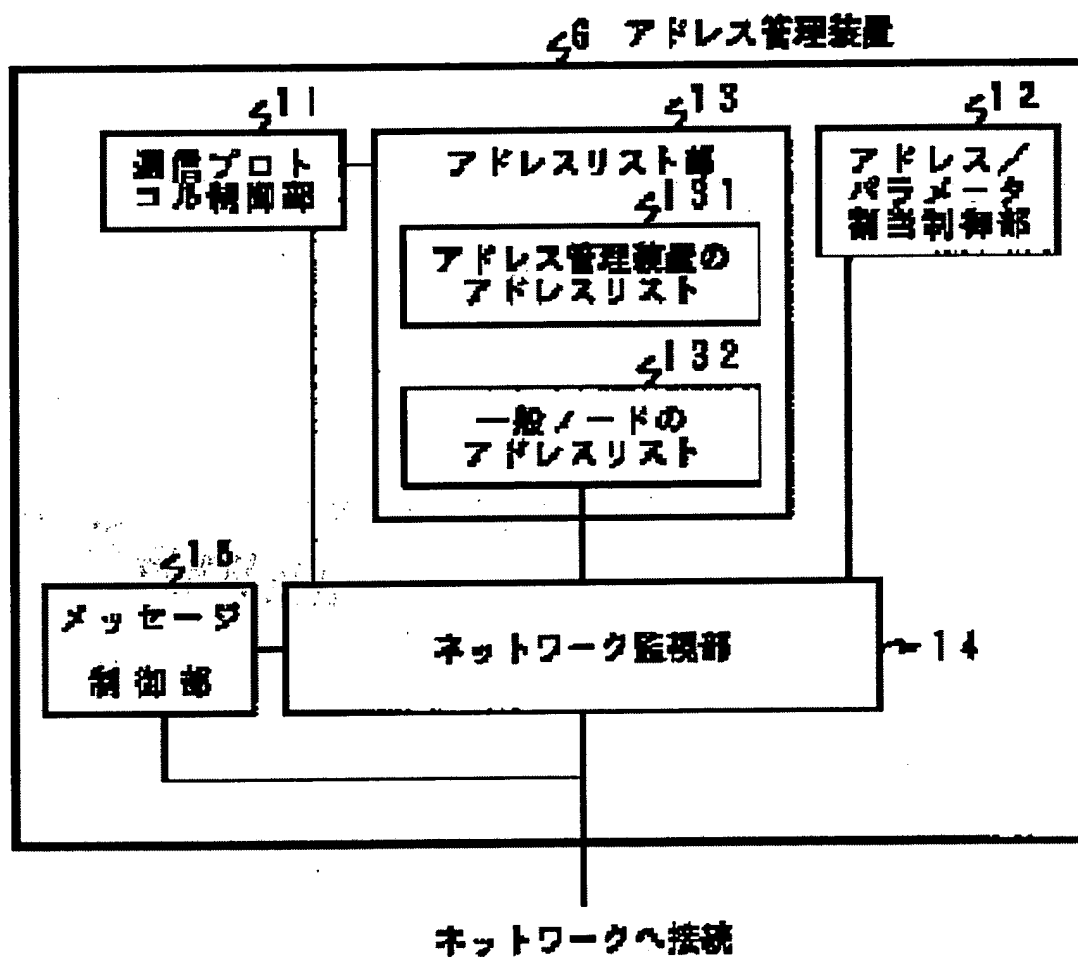
- 44.3 (COMMUNICATION--- Telegraphy)
- 45.2 (INFORMATION PROCESSING--- Memory Units)

Abstract:

PURPOSE: To monitor the existence of unauthorized address managing device and terminal equipment by storing a pair of regular network layer address(NAD) and data link layer address(DAD) and collating whether or not the NAD and DAD described on a packet being transmitted on a network are stored ones.

CONSTITUTION: A network monitoring part 14 fetches the packet running on the network, and judges whether or not the packet is that of DHCPoffer message by observing the OP field of a DHCP message in which a VDP data field is housed. When it is a DHCPoffer, an address managing network layer address from which the message is sent out is read out from the giaddr field or giaddr field of a DHCP message, and it is checked whether or not the address is already registered on an address list 131, and when it is not registered, it is assumed that the unauthorized address managing device exists in the network, then, the effect is reported to a network manager, and a countermeasure is taken.

This Page Blank (uspto)



JAPIO

© 2003 Japan Patent Information Organization. All rights reserved.

Dialog® File Number 347 Accession Number 5231069

This Page Blank (uspto)